1 Enterprise Risk Management in Public Retirement Systems

by Rick Funston and Randy Miller, May 5, 2014

Introduction

This is the first in a series of articles about developing and sustaining an enterprise risk management (ERM) process in public retirement systems. Such systems include investment boards, benefits administration agencies and integrated retirement systems which manage both investments and administer benefit programs. This article addresses the need and some of the challenges these systems face in setting up an effective ERM process.

There are many risks facing public defined benefit retirement systems. Some scenarios being considered include: What if benefit plans become closed and accept no new members? What if they were required to offer multiple plans which include hybrid and/or DC plans for different segments of members? What if case law modified vested rights? What if plans were unable to raise/collect higher employer contributions because they were either unwilling and/or unable to do so? What if significant numbers of employers go bankrupt? What if major investment governance or control failures and associated major losses trigger a loss of confidence in plan administrators resulting in takeovers or a diminution of authorities?

From the perspective of investment performance, what if the equity risk premium no longer exists, or if private equity does not return a premium compared to public equity? What if emerging markets do not return more than developed markets, or financial markets do not perform as expected and the fund significantly under-performs compared to benchmarks? What if correlations between major asset classes become unstable or limits are imposed on

investment in broad asset categories? What if the system fails to meet its investment objectives and the plan fails or funded status drops below 40%?

Conventional risk management efforts are often designed to manage risk when conditions are "normal" or when it is "business as usual" but not when it is extreme, which is unfortunately when risk management is most needed. Conventionally risks have often been managed in silos with each silo having its own language of risk, risk tolerances, assessment criteria and mitigation methods. Typically, siloed risk management is not tied into core decision-making processes, there are uneven risk management capabilities, and different risk management practices, policies and procedures may exist across the organization.

In light of these and other risk scenarios, boards[1] and executives are increasingly asking:

- How prepared are we for the risks and opportunities that inevitably lie ahead?
- How can we find the unexpected before it finds us?
- How can the board get reasonable assurance from management that there are capable people, processes and systems in place to manage the system including the associated risks?
- How can the board get independent reassurance that management's assurances can be relied upon?
- What is the most appropriate balance of roles and responsibilities between board and executive when it comes to risk oversight and risk management?

In response, a growing number of systems are in various stages of either considering or implementing a more integrated and holistic approach to risk management. Frequently, these approaches are referred to as enterprise risk management or ERM. However, a successful process is not only enterprise-wide but also enterprise-deep and becomes part of everything everyone does every day, not just a 'check the box' exercise.

Risk management also needs to be risk intelligent. A diet of pure risk aversion is a recipe for disaster just as much as swinging for the fences at every opportunity. The goal is to build calculated risk taking into the organization and become risk intelligent. While each retirement system is unique and likely at a different stage of capability development, they are typically wrestling with some common questions and issues.

[1] Throughout this article we refer to the board as this is the most common governance structure. This term may be used interchangeably with terms such as commission, i.e., where there is more than a sole fiduciary.

Common questions

- What is the job of a Chief Risk Officer (CRO) or Director of ERM?
- Who should a risk director or CRO report to?
- What is the difference between risk oversight and risk management?
- What is the difference between reasonable assurance and independent reassurance?
- How does ERM relate to investment risk?
- How do you get participation across functions who often have very different definitions of risk and different risk tolerances?

This article attempts to shed some light on the benefits and challenges faced by public retirement systems in developing and deploying such an ERM process.

The Role of the ERM Director / CRO

One of the first steps organizations often take in setting up an ERM program is to appoint a director of ERM or Chief Risk Officer (CRO). What are their responsibilities? Who should they report to? As always, the answer is… "it depends". The reporting relationship depends on their responsibilities. Are they primarily responsible for risk management as a member of operating management or are they primarily responsible for developing organizational risk management capabilities, e.g., its policies, people, processes and systems, and providing independent reassurance?

In private sector financial institutions, CROs are often responsible for managing credit risk and market risk. As such, the private sector CRO is a member of operating management and should provide reasonable but not absolute assurances that relevant risks are being appropriately managed. In this case, the CRO typically reports directly to the CEO and may have a dotted line relationship to the board and/or, if it exists, its risk committee.

In public sector organizations, the CRO or Director of ERM is usually not responsible for risk management and does not have an operational management role. In this role, the individual is responsible for developing enterprise-wide capabilities and providing independent reassurance that operating management's reports can be relied upon. Often the individual reports directly to the Audit and/or Risk Committee as retirement systems are increasingly expanding the scope of the Audit Committee to include enterprise risk.

Here the individual has a dotted line reporting relationship to the CEO or Executive Director. In this case, it is clearly operating management that is responsible for risk identification and risk management and related assurances not the CRO. The CRO or Director of ERM can provide

value to operating management by developing ways to acquire, aggregate and distill risk reporting across the organization to improve risk intelligent decision-making by both the board and executive. ERM can also provide support by developing policies and processes to assist operating management further develop its capabilities.

As it relates specifically to investment risk management, larger retirement systems tend to have their own risk management functions housed within the investment office. This function typically reports to the CIO and is part of operating management and control. The ERM function can help to incorporate the investment risk management reports into the enterprise view.

Typically, a CRO's key responsibilities would include:

- Facilitating a risk intelligent dialogue between board and the executive;
- Developing capable people, processes and systems through training, process improvement and evaluation of potential system upgrades;
- Developing a common language of risk and common tools;
- Recommending to the executive and board risk management policies including risk appetite and risk tolerance;
- Providing independent reassurance to the board that management's reports are reliable;
- Harmonizing, synchronizing and rationalizing existing risk management functions and practices to improve effectiveness and efficiency; and,
- Surfacing inter-dependencies that may not otherwise be recognized.

Risk Oversight and Risk Management

One of any retirement system's biggest sources of risk lies in its asset allocation decision and the related risks and rewards. This decision is a major risk management responsibility of the board and is addressed in a separate article " Strategic Risk". Several other key risks are directly within the purview of the board, for example, the recruitment, selection and compensation or termination of the CEO or Executive Director. One of the first steps in establishing a successful

ERM process is to clearly define the risks that are the responsibility of the board to manage vs. the executive.

The board as a whole is also responsible for risk oversight, i.e., ensuring there are capable people, processes and systems in place to effectively manage the system and the associated risks such that results are achieved and risk exposures are acceptable. To fulfill their responsibilities, they need reasonable (but not absolute) assurances from executives that the system is properly managed and risk exposures are acceptable.

Reasonable Assurance and Independent Reassurance

The board also requires reassurance from parties independent of management that management's assurances can be relied upon. Independent reassurance means that the person responsible for managing the risk and providing assurances cannot also be responsible for an independent assessment of the reliability of those assurances.

As mentioned earlier, a growing number of systems are expanding the role of the Audit Committee to include enterprise risk in order to improve their oversight. This is appropriate for understanding inter-dependencies. However, other committees of the board should retain responsibility for oversight of risk within their respective charters. For example, HR and Compensation Committees should still be concerned about oversight of HR risks as should the Investment Committee be concerned about oversight of investment risks.

Performance and Process

The next challenge is then getting and sustaining active board and executive buy-in and support for the process not just the concept. Again, this cannot be achieved by a mere 'check the box' approach to risk. The key is to hold operating management accountable and quickly demonstrate value. Understandably, a lot of organizations who begin an ERM effort focus on the framework and getting the process in place.

Typically, each function within the organization (e.g., Investment, Legal, HR, IT) has a different view of risk, different risk tolerances and different metrics. Developing a common language is important but unfortunately, this often takes a great deal of time and a lot of reiteration to develop a common understanding. This is discussed further in Part 3 of this series.

Too often the initial focus is on the ERM process and not on the risks themselves. The longer it takes to put an effective process in place, the more likely it is that board members and executives alike will question its value. In the meantime, the organization still has to address the reality of the risks it faces every day, executives are still responsible for successfully managing those risks and fiduciaries are always ultimately accountable.

A more balanced approach would be to start with both risk management performance and the ERM process simultaneously. What are the key risks? Who is responsible for managing them? Where are the vulnerabilities? What are the priorities?

Dialogue not just reports

As John Maynard Keynes once said "it is better to be roughly right than precisely wrong." The most important part of an ERM program is the dialogue it creates between the board and executives. It is much less about crafting perfect policy than it is about getting the right focus on exposures and clarifying risk management accountabilities.

Start with a discussion of the most important risks the organization faces, clarify who is responsible, understand what are they doing about those risks and whether there are any unacceptable residual exposures. Even if it is roughly framed, a dialogue to improve understanding of the major risks and responsibilities for managing them is an essential first step. Then the stage is set to move to a discussion of how to improve the organization's awareness and capabilities to more successfully manage, and improve its ability to monitor and report on priority risks. Such capabilities range from risk identification and assessment to management and reporting.

The responsibility for risk management and risk reporting must clearly rest with executive management who in turn deploy risk intelligent management throughout the organization. While ERM can support operating management, it is operating management who must clearly own the risks and report on them. ERM directors may also fall into the trap of presenting the risk report or dashboard and thus the accountability tends to shift to the ERM process away from operating management.

Boards too often tend to accept a risk report at face value and file it away as an end in itself rather than using the report as a starting point for a dialogue with operating management. Successful ERM can't be a stand-alone process. It has to be part of the way the organization does business, enterprise-wide and enterprise-deep.

The next article in this series discusses how to kick start the dialogue on risk.

About the authors. Rick Funston is the Managing Partner of Funston Advisory Services LLC which specializes in governance, strategy, and risk intelligence. Rick was formerly the National Practice Leader for Deloitte's Governance and Risk Oversight Services. He is the principal author of 'Surviving and Thriving in Uncertainty: Creating the Risk intelligent Enterprise" Wiley and Sons, 2010.

Randy Miller is a Principal of Funston Advisory Services LLC and former senior consulting partner with Deloitte for 27 years with extensive experience in strategy, benchmarking and operations improvement.

www.funstonadv.com